Introdução aos Reticulados Ideais

Cintya Wink de Oliveira Benedito* **Antonio Aparecido de Andrade†**
Departamento de Matemática, IBILCE, UNESP,
15054-000, São José do Rio Preto, SP
E-mail: cwinktc@hotmail.com, andrade@ibilce.unesp.br.

RESUMO

Neste trabalho apresentamos o conceito de reticulados ideais e suas principais propriedades, onde também apresentamos algumas propriedades importantes de alguns reticulados especiais no $\mathbb{R}^n$. Apresentamos também dois conceitos importantes nesta teoria que são a diversidade de um reticulado e a distâcia produto mínima.

Assim, sejam $\mathbb{K}$ um corpo de número de grau n tal que $\mathbb{K}$ é totalmente real, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$, $\alpha \in \mathbb{K}$ tal que $\alpha_i = \sigma_i(\alpha) > 0$, para todo $i = 1, \ldots, n$ e $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$, onde $\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$, onde $\sigma_i : \mathbb{K} \to \mathbb{C}$, para $i = 1, \ldots, n$, são os monomorfismos de $\mathbb{K}$, é uma perturbação do homomorfismo canônico. Se tomarmos $M \subset \mathbb{K}$ um $\mathbb{Z}$-módulo livre, temos que $\sigma_\alpha(M)$ é um reticulado do $\mathbb{R}^n$.

Sejam ϕ uma involução e $\mathbb{F} = \{x \in \mathbb{K} | \phi(x) = x\}$ o corpo fixo da involução. Se $\mathcal{I} \subseteq \mathbb{K}$ é um ideal fracionário e $\alpha \in \mathbb{F}$ tal que $\alpha\mathcal{I}\phi(\mathcal{I}) \subseteq \mathcal{D}_{\mathcal{O}_{\mathbb{K}}|\mathbb{Z}}{}^{-1}$, onde $\mathcal{D}_{\mathcal{O}_{\mathbb{K}}}$ é o discriminante de $\mathbb{K}$, então, definimos **ideal reticulado** por $\Lambda = (\mathcal{I}, b_\alpha)$, onde a função $b_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}$ é tal que $b_\alpha(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha x\phi(y))$ para todo $x, y \in \mathcal{I}$.

Temos que o **determinante** de b_α será dado pelo determinante da matriz $(b_\alpha(v_i, v_j))_{i,j=1}^n$, onde $\{v_1, \ldots, v_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$.

Dizemos que um reticulado ideal $(\mathcal{I}, b_\alpha)$ é **par** se $b_\alpha(x, x)$ é um número par para todo $x \in \mathcal{I}$. Caso contrário dizemos que é **ímpar**. E, dizemos que ele é **positivo** se $b_\alpha(x, x) > 0$ para todo $x \in \mathcal{I}$ tal que $x \neq 0$. Neste caso, o mínimo de $(\mathcal{I}, b_\alpha)$ é definido por $min(\mathcal{I}, b_\alpha) = min\{b_\alpha(x, x);\ x \in \mathcal{I},\ x \neq 0\}$.

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. A **diversidade** de Λ é definida por

$$div(\Lambda) = min\{div(x) :\ x \in \Lambda,\ x \neq 0\},$$

onde $x = (x_1, \ldots, x_n)$ e $div(x) = \sharp\{i : x_i \neq 0\}$, onde $\sharp(A)$ é o número de elementos do conjunto A.

Proposição 0.1. *Seja $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Um reticulado ideal $\Lambda = (\mathcal{I}, b_\alpha)$ tem diversidade $div(\Lambda) = r_1 + r_2$, onde r_1 é a quantidade dos monomorfismos reais de $\mathbb{K}$ e r_2 a metade dos monomorfismos imaginários de $\mathbb{K}$.*

Proposição 0.2. *Seja $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Um reticulado ideal $\Lambda = (\mathcal{I}, b_\alpha)$ pode ser imerso no $\mathbb{R}^n$ com*

- *diversidade n se $\mathbb{K}$ é totalmente real,*
- *diversidade $\frac{n}{2}$ se $\mathbb{K}$ é totalmente complexo.*

*Aluna de Mestrado - Bolsista Fapesp
†Orientador

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n. A **distância produto mínima** do reticulado é definido por

$$d_{p,min}(\Lambda) = min_{x\in\Lambda} d_p(x),$$

onde $x = (x_1, \ldots, x_n)$ e $d_p(x) = \prod_{i=1}^{n} |x_i|$.

Teorema 0.1. *Se $\mathbb{K}$ é um corpo de números totalmente real de grau n com discriminante $\mathcal{D}_{\mathbb{K}|\mathbb{Q}}$ e $\mathcal{I}$ um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{I}, b_\alpha)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(b_\alpha)}{|\mathcal{D}_{\mathbb{K}|\mathbb{Q}}|}} min(\mathcal{I}),$$

onde $min(\mathcal{I}) = min_{o\neq y\in\mathcal{I}} \frac{|\mathcal{N}_{\mathbb{K}|\mathbb{Q}}(y)|}{\mathcal{N}(\mathcal{I})}$.

Corolário 0.1. *Se $\mathbb{K}$ é um corpo de números totalmente real de grau n e $\mathcal{I}$ um ideal prncipal de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{I}, b_\alpha)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(b_\alpha)}{|\mathcal{D}_{\mathbb{K}|\mathbb{Q}}|}}.$$

Palavras-chave: *reticulados, reticulado ideal, homomorfismo canônico, diversidade, distâcia produto mínima*

Referências

[1] G.C. Jorge, **Reticulados Ideais via corpos abelianos**. 2008, 176f. Tese (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[2] F. Oggier, **Algebraic methods for channel coding**. 2005, 125f. Tese (Doutorado em Matemática e informática), École Polytechnique Fédeérale de Lausanne, Lausanne, 2005.

[3] C.M. Oliveira, **Discriminante, Ramificação e Diferente**. 2005, 131f. Tese (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[4] P. Samuel. **Algebraic theory of numbers**. Paris: Hermann, 1970.